UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	Case No. CR19-159-RSL ORDER GRANTING IN PART THE GOVERNMENT'S CONSOLIDATED MOTIONS *IN LIMINE*

This matter comes before the Court on the government's "Consolidated Motions *in Limine*" (Dkt. # 282). Having reviewed the submissions of the parties and the remainder of the record, the Court finds as follows:

I. BACKGROUND

Defendant Paige Thompson faces trial for charges of wire fraud, violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) ("CFAA"), access device fraud, and aggravated identity theft. Dkt. # 166. The indictment alleges that defendant created proxy scanners that allowed her to identify Amazon Web Services servers with misconfigured web application firewalls that permitted outside commands to reach and be executed by the servers. Id. at ¶ 12. Defendant then allegedly sent commands to the misconfigured servers to obtain security credentials for particular accounts or roles belonging to the victims. Id. at ¶¶ 11-13, 16-18. Defendant allegedly used these "stolen credentials" to "copy data, from folders or buckets

of data" in the victims' cloud storage space and set up cryptocurrency mining operations on the victims' rented servers. Id. at ¶¶ 14-15, 21.

II. DISCUSSION

The government moves the Court to: (A) exclude evidence or argument regarding potential or actual cyber-security vulnerabilities of victim companies, including Capital One, other than the vulnerability allegedly exploited by defendant, (B) exclude evidence or argument regarding a note given to an Amazon employee by an unknown person in mid-to-late May 2019, describing a potential Amazon Web Services ("AWS") security vulnerability, (C) exclude evidence relating to an $80 million civil penalty imposed against victim Capital One by the Office of the Comptroller of the Currency ("OCC") in August 2020, (D) exclude evidence regarding a pending $190 million settlement by Capital One of a class-action lawsuit brought on behalf of Capital One's customers whose personal identifying information ("PII") defendant allegedly stole, and (E) exclude evidence and argument from defendant's mental health expert except as it bears directly on her capacity to form the specific intent for the crimes for which she is being tried. Dkt. # 282 at 1-2. The Court considers each motion *in limine* in turn.

A. Motion *in Limine* No. 1: Victim Security Vulnerabilities

The government moves the Court to exclude evidence regarding cyber-security vulnerabilities at Capital One or other victim entities that are unrelated to the specific vulnerability that defendant allegedly exploited in the case at hand. The government argues that such evidence would be irrelevant and would confuse the issues, mislead the jury, waste time, and risk unfair prejudice. Dkt. # 282 at 2 (citing Fed. R. Evid. 401-403). In particular, the government argues that such evidence would be irrelevant because the existence of other vulnerabilities does not "bear on any issue involving the elements of the charged offense[s]." Id. at 2 (quoting United States v. Dean, 980 F.2d 1286, 1288 (9th Cir. 1992)).

The Court disagrees with the government. The government's argument is hung on the legal proposition that victim negligence is not a defense to wire fraud. The government, however, makes an unsupported leap to the conclusion that victim negligence is also not a

defense to CFAA violations, and the security vulnerability evidence must therefore be excluded as irrelevant.

In the CFAA context, evidence that access to a computer was open to the general public is highly relevant. See hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1197-98 (9th Cir. 2022) ("The CFAA contemplates the existence of three kinds of computer systems: (1) computers for which access is open to the general public and permission is not required, (2) computers for which authorization is required and has been given, and (3) computers for which authorization is required but has not been given."). Further, the Ninth Circuit has implied that computer access may be deemed open to the general public even if a particular access *method* is restricted. See id. at 1185, 1186, 1201 (acknowledging that LinkedIn took technological steps to protect the data on its website from the scraping engaged in by hiQ, but nonetheless finding that access was open to the general public where LinkedIn profiles were "made visible to the general public"). Therefore, under Rules 401 and 402, evidence of security vulnerabilities apart from the one that defendant allegedly utilized is relevant and admissible to the CFAA charges for accessing a computer without authorization because it conceivably goes to whether access to the computer was open to the general public. Because this evidence may be highly relevant, it likewise passes Rule 403's balancing test.

Regarding the wire fraud charge, the government is correct that victim negligence is not a defense to wire fraud. United States v. Lindsey, 850 F.3d 1009, 1015 (9th Cir. 2017) ("We join several of our sister circuits in holding that a victim's negligence is not a defense to wire fraud.").[1] Evidence of victim negligence is thus irrelevant to the wire fraud charge. See United

[1] Defendant argues that Lindsey should be read as limited to the mortgage fraud context. See Dkt. # 292 at 3. It is true that Lindsey involved wire fraud of the mortgage fraud variety. However, limiting its holding to that ambit would create an absurd result where mortgage fraud materiality is objective, while other types of wire fraud require subjective materiality, even though all are hung on the same statute, 18 U.S.C. § 1343. The Ninth Circuit's opinion in Lindsey does not allude to this intent, and its analysis is based in United States v. Ciccone, 219 F.3d 1078 (9th Cir. 2000), a wire fraud case that involved fundraising fraud. See Lindsey, 850 F.3d at 1015 (citing Ciccone, 219 F.3d at 1083).

States v. Click, 807 F.2d 847, 850 (9th Cir. 1987) (Relevant evidence "must be probative of the proposition it is offered to prove, and . . . the proposition to be proved must be one that is of consequence to the determination of the action."). Therefore, to the extent that defendant seeks to introduce evidence regarding cyber-security vulnerabilities at Capital One or other victim entities unrelated to the specific vulnerability that defendant allegedly exploited here to show victim negligence as a defense to wire fraud, she may not do so.

Defendant argues that "Lindsey fully permits the defense to introduce evidence of cybersecurity industry standards and make inferential arguments from such evidence." Dkt. # 292 at 4 (citing Lindsey, 850 F.3d at 1016-17). The Court agrees that Lindsey permits defendant to introduce evidence of industry standards to disprove objective materiality. See Lindsey, 850 F.3d at 1016. This, however, allows in evidence of industry practices generally, not victim practices generally, and it is unclear to the Court how evidence of victim vulnerabilities other than the one that defendant allegedly exploited would be relevant to this argument.

Defendant also argues that "[t]he question of whether the information was essentially public is also relevant as to whether Ms. Thompson had the requisite intent to defraud the alleged victims." Dkt. # 292 at 3. Defendant's arguments to this point, however, go to whether access was "without authorization," which is a question relevant to the CFAA, not to wire fraud. See id. The Court is therefore unable to resolve this issue at this time.

Finally, defendant argues that evidence of the victims' prior cybersecurity vulnerabilities is relevant "to dispel the government's allegation that Ms. Thompson copied 'confidential business information.'" Dkt. # 292 at 4. Defendant's argument to this point is made without context. However, the Court understands this argument to go to whether the data that defendant allegedly downloaded qualifies as property under the wire fraud statute. See Dkt. # 202 at 7-9. "Confidential business information has long been recognized as property," and accordingly meets the "property" requirement in the wire fraud statute. Carpenter v. United States, 484 U.S. 19, 25-26 (1987). In Louderman, the Ninth Circuit found that "confidential internal information

concerning telephone customers or post office box holders" was property under the wire fraud statute where "the object of the scheme to defraud here was . . . to obtain intangible, commercial information which the telephone company and post office chose to keep confidential and which its customers expected would remain confidential." United States v. Louderman, 576 F.2d 1383, 1386-87 (9th Cir. 1978). Therefore, to the extent that defendant seeks to introduce evidence of the victims' prior cybersecurity vulnerabilities to argue that the data was not "confidential business information," she may do so, but only if such evidence goes to the specific data that defendant allegedly obtained in this case. Evidence that *other* data was not confidential business information due to security vulnerabilities would be irrelevant.

B. Motion *in Limine* No. 2: AWS Security Vulnerability Note

The government moves the Court to exclude evidence regarding "a handwritten note of unknown origin given to an Amazon employee at an internal Amazon conference in May, 2019, and then shared by Amazon with Capital One." Dkt. # 282 at 5-6. The note warned Amazon of an open SOCKS proxy. Id. at 6. The government argues that the note is irrelevant because: (i) the security vulnerability that defendant allegedly exploited in this case did not involve a SOCKS proxy, (ii) Amazon received the note approximately two months after defendant allegedly exfiltrated Capital One's data, and (iii) the government is unaware of any evidence that defendant was involved with the writing or dissemination of the note. Id.

Defendant argues that the note is relevant because it identifies the same IP address that defendant allegedly accessed and the same vulnerability that defendant allegedly exploited and because there is circumstantial evidence that Capital One believed that defendant authored or otherwise authorized the note. See Dkt. # 292 at 5-6. Further, defendant avers that the government's argument that the note is unrelated to defendant because that the note refers to a SOCKS proxy while defendant allegedly used an HTTP proxy is disingenuous because the two proxy types are regularly conflated or confused and may be utilized together. See id. at 6. Finally, defendant argues that the fact that Capital One received the note two months after defendant allegedly exfiltrated Capital One's data is irrelevant because defendant allegedly

accessed the same server shortly after Capital One received the note – which could indicate that she was trying to see if Capital One had resolved the security vulnerability after receiving her note – and because May 2019 is well within the indictment's scope of March 2019 through August 2019. Id. at 7.

In light of the substantial similarities between defendant's alleged conduct and the vulnerability described in the note, the Court rejects the government's argument that the note is irrelevant because it refers to a SOCKS proxy rather than an HTTP proxy. The Court is likewise unpersuaded that the date of the note renders it irrelevant, given its proximity to defendant's alleged conduct.

C. Motion *in Limine* No. 3: Capital One Civil Penalty

The government moves the Court to exclude evidence of the fact that the OCC imposed an $80 million fine on Capital One following defendant's alleged breach. Dkt. # 282 at 8. In particular, the government argues that the Court should exclude all evidence relating to the imposition of the penalty pursuant to Federal Rules of Evidence 401 and 403 and should exclude the OCC consent order itself as hearsay. Id. Defendant argues that evidence of the OCC fine is critical to its cross-examination of Capital One witnesses, as Capital One has a strong interest in blaming the data breach on defendant. See Dkt. # 292 at 7. Defendant further argues that the consent order is not hearsay because it is falls under the public record exception to the hearsay rule. See Dkt. # 292 at 8-9.

The Court agrees with defendant that evidence of the OCC fine is relevant cross-examination evidence, and this use outweighs the danger of unfair prejudice, confusing the issues, and misleading the jury. See Fed. R. Evid. 403. The Court therefore declines to exclude evidence of the OCC fine pursuant to Rules 401 and 403.

The Court next considers if the OCC consent order is excludable hearsay. "'Hearsay' means a statement that (1) the declarant does not make while testifying at the current trial or hearing; and (2) a party offers in evidence to prove the truth of the matter asserted in the statement." Fed. R. Evid. 801(c). There is an exception to the rule against hearsay for "[a]

record or statement of a public office if . . . it sets out . . . factual findings from a legally authorized investigation." Fed. R. Evid. 803(8)(A)(iii). The OCC is a public office, and the consent order sets out the OCC's factual findings. See Dkt. # 282-1 at 3-4. The OCC consent order therefore fulfills this requirement and is not inadmissible hearsay.

D. Motion *in Limine* No. 4: Capital One Class Action Settlement

Pursuant to Federal Rules of Evidence 401, 403, and 408, the government moves the Court to exclude all evidence relating to Capital One's proposed $190 million class action settlement stemming from the data breach. Dkt. # 282 at 10-11.

First, the government argues that because the only thing the class action settlement could potentially prove is Capital One's negligence (and other wrongdoings), it is irrelevant, and the Court should therefore exclude it pursuant to Rule 401. Id. at 11. As explained above, supra Part II.A., the Court disagrees that such evidence is inadmissible across the board. The Court therefore declines to exclude the settlement on this ground.

Second, the government argues that any probative value of the evidence would be substantially outweighed by the danger of unfair prejudice, confusion of the issues, and misleading the jury, and the Court should therefore exclude it pursuant to Rule 403. Dkt. # 282 at 11. The government argues this is true for three reasons: first, Capital One did not admit to any wrongdoing in the settlement, so it would therefore be impossible for the jury to discern the facts that lead to it. Id. Second, the settlement is for a very large sum - $190 million – and this sum alone may mislead and confuse the jury into believing that Capital One, not defendant, was at fault. Id. at 11-12. Finally, the legal claims addressed in the settlement are distinct from those in the indictment, and therefore may mislead and confuse. Id. at 12. The defense does not confront the government's arguments regarding Rule 403.

The Court agrees that the proposed settlement is properly excluded under Rule 403. Under Rule 403, "The court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence."

Fed. R. Evid. 403. A settlement is not a reliable indicator of misconduct, and the jury may be unduly swayed by the large amount of money involved and the fact that Capital One agreed to the settlement. Accord In re Tenet Healthcare Corp. Sec. Litig., No. CV 02-8462-RSWL(RZX), 2007 WL 5673884, at *2 (C.D. Cal. Dec. 5, 2007). The settlement is therefore unduly prejudicial under Rule 403.

Because the Court concludes that evidence of the proposed class action settlement is properly excluded pursuant to Rule 403, the Court does not consider the parties' arguments pursuant to Rule 408.

E. Motion *in Limine* No. 5: Mental Health Evidence

The government moves the Court to exclude evidence regarding defendant's mental health unless such evidence relates directly to defendant's *mens rea* for the charged offenses. Dkt. # 282 at 12-13. Defendant argues that this motion should be denied as premature because defendant has not yet decided if she will put on a mental condition defense. See Dkt. # 292 at 9-11.

The Court agrees with the government. Only relevant evidence is admissible. Fed. R. Evid. 402. "Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action." Fed. R. Evid. 401. A fact is of consequence to the determination of the action if it "bear[s] on any issue involving the elements of the charged offense." Dean, 980 F.2d at 1288. Evidence of defendant's mental health only conceivably bears on the intent elements of the charged offenses. Such evidence offered for any other purpose is therefore inadmissible. The Court, therefore, grants the government's motion to exclude irrelevant mental health evidence.

III. CONCLUSION

For all of the foregoing reasons, IT IS HEREBY ORDERED that government's Consolidated Motions in Limine (Dkt. # 282) are GRANTED IN PART and DENIED IN PART.

1. Motion *in Limine* No. 1 is GRANTED IN PART. Defendant may present evidence regarding cyber-security vulnerabilities at Capital One or other victim entities that are unrelated to the specific vulnerability that defendant allegedly exploited in the case at hand to the extent that defendant seeks to show that access to the computer was open to the general public. Defendant may not present such evidence to show victim negligence in relation to the wire fraud charge.
2. Motion *in Limine* No. 2 is DENIED. Defendant may present the AWS security vulnerability note.
3. Motion *in Limine* No. 3 is DENIED. Defendant may use the OCC fine as cross-examination evidence, and the OCC consent order is not excludable hearsay.
4. Motion *in Limine* No. 4 is GRANTED. The Court excludes all evidence relating to Capital One's proposed $190 million class action settlement stemming from the data breach.
5. Motion *in Limine* No. 5 is GRANTED. Defendant's mental health evidence is excluded unless it relates to defendant's *mes rea* for the charged offenses.

DATED this 7th day of June, 2022.

Robert S. Lasnik
United States District Judge